IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF: **10106 BOSWORTH CT.,** **BETHESDA, MARYLAND 20817**	**Case No. 24-mj-540-AAQ** **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent Jeremy Kiser, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for **10106 Bosworth Ct., Bethesda, Maryland 20817** ("the **PREMISES**"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so employed for approximately eighteen years. As an HSI Special Agent, I have successfully completed the twelve-week Criminal Investigator Training Program ("CITP") at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. At the conclusion of CITP, I completed an additional twelve-week program with FLETC's Immigration and Customs Enforcement Special Agent Training Academy. As part of my training at FLETC, I received

extensive instruction in the areas of immigration law, customs law, firearms training, interview techniques, and the Federal Rules of Evidence.

3. As a Special Agent with HSI, my duties include, among other things, the investigation of criminal violations of U.S. import and export law, including violations of the AECA, ITAR, ECRA, and EAR. Additionally, I am familiar with federal criminal laws related to the unlawful export of arms and commodities from the United States, as determined by the Department of State ("DOS"), Directorate of Defense Trade Control ("DDTC"); the Department of Commerce ("DOC"), Bureau of Industry and Security ("BIS"); and the Department of Treasury, Office of Foreign Asset Controls ("OFAC"), as these agencies have statutory responsibility and authority to regulate exports. Moreover, as an HSI Special Agent, I am generally authorized to investigate violations of U.S. laws, to execute search and seizure warrants, and to swear to complaints issued under the authority of the United States.

4. The statements set forth in this affidavit are based on my investigation to date, including undercover communications, observations, and review of information provided to me by other law enforcement officers and individuals involved in the investigation. I also relied on my training, experience, and background in law enforcement in evaluating this information. Because this affidavit is being submitted for the limited purpose of establishing probable cause

for a search warrant, I have not included every fact or source of information establishing violations of federal law.

5. This Court has venue and jurisdiction to issue the proposed warrants under Federal Rule of Criminal Procedure 41(b)(1) and (b)(3).

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Peter Biar Ajak ("**Ajak")**, Abraham Chol Keech ("**Keech")**, and other co-conspirators, have violated 22 U.S.C. § 2778(c); 22 C.F.R. Parts 121.1, 123.1, 127.1(a)(4), 127.3 (Conspiracy to Violate the Armed Export Controls Act and the International Traffic in Arms Regulations); 50 U.S.C. § 4819(a)(1), (a)(2)(D), and (b); 15 C.F.R. Parts 736.2(b)(1), 774, Supp. No. 1 (Conspiracy to Violate the Export Control Reform Act and the Export Administration Regulations); and 18 U.S.C. § 554(a) (Smuggling Goods from the United States), by purchasing export-controlled weapons and attempting to export these items

from the United States to South Sudan without first obtaining the required licenses from the U.S. government.

7. Based on the facts set forth below, I respectfully submit that probable cause exists to believe that the requested warrant for the **PREMISES** will lead to evidence, fruits, and/or instrumentalities of those violations.

LEGAL BACKGROUND

8. To further national security and foreign policy interests of the United States, Congress and the President control and regulate the export from the United States of arms, other defense articles, and certain goods and services. Several federal statutes impose limitations and licensing requirements on the export or transfer of these items from the United States to a foreign country or national. The export control and sanctions law relevant to this case are further described below.

The Arms Export Control Act and the International Traffic in Arms Regulations

9. The AECA authorizes the President to regulate and control the export of defense-related articles. To that end, the AECA establishes a United States Munitions List ("USML"), which identifies and defines the defense articles subject to export controls, and provides for

criminal penalties for any willful violation of the AECA or any rule or regulation thereunder. See 22 U.S.C. § 2778(a)-(c).

10. The United States Department of State, through the Directorate of Defense Trade Controls ("DDTC"), implements these statutory provisions through the ITAR, 22 C.F.R. Parts 120-130. The ITAR contains the USML, which sets forth twenty-one categories of "defense articles" that are subject to export licensing controls by the DDTC, ranging from firearms parts to military equipment to missiles. 22 C.F.R. Part 121.1. As relevant here, (1) AK-47 rifles (fully automatic), (2) PKM rifles (fully automatic), (3) RPG-7 grenade launchers, (4) PG-7 HE rounds; (5) FIM-92 Stinger missile systems; (6) M-67 hand grenades, and (7) PG-7VT / PG-7T AT rounds are designated as defense articles on the USML.

11. The ITAR defines an "export" as, among other things, the sending or taking of a defense article out of the United States in any matter. 22 C.F.R. Part 120.50(a). Unless an exemption applies, the AECA and the ITAR prohibit all defense articles from being exported from the United States without a license or other approval from the DDTC. 22 U.S.C. § 2778(b)(2); 22 C.F.R. Part 123.1. Registration with DDTC is "generally a precondition to the issuance of any license or other approval" to export defense articles. 22 C.F.R. Part 122.1(c).

12. Pursuant to the ITAR, it is unlawful for any person, without first obtaining a license or other written approval from DDTC, to "conspire to export … or cause to be exported

… any defense article, technical data, or defense service for which a license or written approval is required." 22 C.F.R. Part 127.1(a)(4).

13. At all times relevant to this investigation, South Sudan was subject to a U.N. Security Council Arms Embargo, as further described below. Accordingly, all transactions that are prohibited under the U.N. Security Council's embargo and involving U.S. persons inside or outside the United States, or any person in the United States, are prohibited under the ITAR unless the Department of State specifies different measures. *See* 22 C.F.R. Part 126.1(c)(1). Specifically, Part 126.1(d)(2) states that the United States has a "policy of denial" for defense articles to South Sudan, and that no "sale, export, [or] transfer" of defense articles may be made without a license from DDTC. Furthermore, "it is the policy of the Department of State to deny licenses and approvals in such cases." 22 C.F.R. Parts 126.1(d), (e), and (w).

14. Pursuant to 22 U.S.C. § 2778(c), "[a]ny person who willfully violates [AECA or ITAR] . . . shall upon conviction be fined for each violation not more than $1,000,000 or imprisoned not more than 20 years, or both." *See also* 22 C.F.R. Part 127.3 (describing penalties for violations of the AECA and ITAR).

The Export Control Reform Act ("ECRA")
and the Export Administration Regulations ("EAR")

15. The ECRA provides, among its stated policy objectives, that "[t]he national security and foreign policy of the United States require that the export, reexport, and in-country

transfer of items, and specific activities of United States persons, wherever located, be controlled." 50 U.S.C. § 4811(2). To that end, the ECRA grants the President the authority to control "(1) the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons; and (2) the activities of United States persons, wherever located," relating to specific categories of items and information. *Id.* at § 4812(b). The ECRA further grants to the Secretary of Commerce the authority to establish the applicable regulatory framework. *Id.* at § 4813(a).

16. Pursuant to the ECRA, the Department of Commerce reviews and controls the export of certain items, including goods (such as firearms and ammunition that are not on the USML), software, and technologies, from the United States to foreign countries through the EAR, 15 C.F.R. Parts 730-774. In particular, the EAR restrict the export of items that could make a significant contribution to the military potential of other nations or that could be detrimental to the foreign policy or national security of the United States. The EAR impose licensing and other requirements for items subject to the EAR to be exported lawfully from the United States or re-exported lawfully from one foreign destination to another.

17. The most sensitive items subject to EAR controls are identified on the Commerce Control List ("CCL"), published at 15 C.F.R. Part 774, Supp. No. 1. Items on the CCL are categorized by an Export Control Classification Number ("ECCN") based on their technical

characteristics. Each ECCN has export control requirements depending on the destination, end user, and end use.

18. As relevant here, (1) PSL sniper rifles; (2) 7.62 x 39 mm ammunition; and (3) 7.62 x 54 mm ammunition are designated under ECCN numbers 0A501.a (firearms) and 0A505.1 (ammunition), respectively. At all times relevant to this investigation, items controlled under these ECCN numbers require a license for export to South Sudan. 15 C.F.R. Part 738, Supp. No. 1.

19. Pursuant to 50 U.S.C. § 4819(a)(1), it is unlawful for anyone to willfully conspire to violate the ECRA or the EAR. *See also* § 4819(a)(2)(D) (making it unlawful to conspire with another person to violate the EAR). Such unlawful acts include, among others, exporting an item subject to the EAR from the United States to another country without a license, if the item is controlled and export to the destination country requires a license. 15 C.F.R. Part 736.2(b)(1).

20. Pursuant to 50 U.S.C. § 4819(b), "[a] person who . . . willfully conspires to commit . . . an unlawful act described in subsection (a)" shall be guilty of a crime and subject to imprisonment of up to 20 years.

Smuggling of Goods from the United States

21. Title 18, United States Code, Section 554, makes it illegal to fraudulently or knowingly buy or in any manner facilitate the transportation or concealment of any item, prior to

exportation, knowing the item is intended for export from the United States in violation of the AECA, ITAR, ECRA, or the EAR. Violations of 18 U.S.C. § 554 are punishable by a prison term of up to 10 years. 18 U.S.C. § 554(a).

BACKGROUND ON SOUTH SUDAN AND THE UNITED NATIONS ARMS EMBARGO

22. South Sudan became an independent nation in July 2011. Following independence, in December 2013, longstanding political tensions between South Sudan's president and first vice president erupted into armed conflict and widespread violence. The parties signed several ceasefire agreements, culminating in an August 2015 peace agreement (the Agreement to Resolve the Conflict in the Republic of South Sudan, or ARCSS), which provided for a Transitional Government of National Unity. A ceasefire generally held from August 2015 to July 2016, when fighting broke out in South Sudan's capital, eventually spreading to the rest of the country. In September 2018, the major warring factions signed a "revitalized" peace agreement (the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan, or R-ARCSS), and in February 2020, the parties formed the Revitalized Transitional Government of National Unity.

23. In July 2018, the United Nations Security Council adopted Resolution 2428 regarding the situation in South Sudan. In that resolution, the Council "[e]xpress[ed] grave alarm and concern regarding the conflict between the Transitional Government of National Unity (TGNU) and opposition forces," which "has resulted in great human suffering, including

significant loss of life, conflict-induced food insecurity and threat of famine, displacement of more than four million people, and the loss of property." Based on its findings, the Council decided that "all Member States shall immediately take the necessary measures to prevent the direct or indirect supply, sale or transfer to the territory of South Sudan from or through their territories . . . of arms and related materials of all types." The Security Council has renewed the South Sudan arms embargo every year since 2018, most recently on May 30, 2023. In the most recent renewal—and to explain the decision to renew the embargo—the Council "[e]xpress[ed] concern over the continued intensification of violence prolonging the political, security, economic, and humanitarian crisis in most parts of the country," "[e]xpress[ed] its alarm and deep concern over continued armed violence against humanitarian workers and facilities," and "[e]xpress[ed] grave concern regarding increased violence between armed groups … which has killed and displaced thousands." In addition, the Council "[e]xpress[ed] grave concern at the

threat to peace and security in South Sudan arising from the illicit transfer, destabilizing accumulation and misuse of small arms and light weapons.

RELEVANT PERSONS AND ENTITIES

24. **Abraham Chol Keech** is a naturalized U.S. citizen originally from South Sudan who currently resides in Utah. As described below in the probable cause statement, he serves as a coordinator for opposition group(s) in South Sudan.

25. **Peter Biar Ajak** is an asylee born in South Sudan and who resides in Maryland. As described below in the probable cause statement, he currently serves as a fellow at a U.S. university and regularly authors articles regarding South Sudan's political and economic future.

26. PERSON-1 is a naturalized U.S. citizen originally from South Sudan who resides in Virginia.

27. PERSON-2 is a Legal Permanent Resident originally from South Sudan who resides in Nebraska. As described below, he serves as a U.S.-based representative of a general with a South Sudanese opposition group.

28. PERSON-3 is a naturalized U.S. citizen who resides in New York.

29. PERSON-4 is a U.S. citizen who works as a marketing and public relations specialist based in New York. PERSON-4 previously worked at the U.S. Department of State. PERSON-4 is also the Registered Agent for "U.S. Company-1," a company that, based on a database search, is a corporation based in New York.

30. PERSON-5 is a U.S. citizen and former U.S. military member who resides in California.

31. PERSON-6 is an individual traveling on a Canadian passport described by **Ajak** as an associate and weapons expert.

PROBABLE CAUSE

32. For over a year, **Keech**, **Ajak**, and others have conspired to purchase AK-47 rifles (fully automatic), PKM rifles (fully automatic), RPG-7 grenade launchers, FIM-92 Stinger missile systems, M-67 hand grenades, PSL sniper rifles, ammunition, and other export-controlled items from undercover law enforcement agents, and to export these items from the United States to South Sudan to arm opposition groups seeking to effect a non-democratic regime change in South Sudan. **Keech** and **Ajak** knew that smuggling the weapons and ammunition out of the country without a license from the U.S. government was illegal and would violate U.S. laws. Nevertheless, in or around February 2024, they caused funds to be transferred to undercover agents through U.S. Company-1 to purchase approximately $4 million worth of munitions and other goods for illegal export to South Sudan. The investigation into this conduct is described more fully in the paragraphs below.

HSI Learns of Efforts to Obtain

Weapons for Individuals in South Sudan

33. In or around September 2021, a cooperating defendant in an unrelated matter[1] received a series of messages via an instant messaging application from an individual using a phone number ending in -9133. Investigators subsequently identified the user of the -9133 phone through law enforcement database checks as PERSON-1. PERSON-1 reached out to the cooperating defendant to explore ways to obtain weapons for a South Sudanese political party and opposition group ("OPPOSITION GROUP-1"). PERSON-1 shared a list of various weapons and ammunition needed by OPPOSITION GROUP-1, and the cooperating defendant provided PERSON-1 with pricing information. The cooperating defendant also introduced PERSON-1 to a "close friend" he/she had "worked with for years on these sensitive issues," who was in fact an undercover law enforcement agent.

34. Over the next year, undercover agents from the United States Department of Defense (UC-1) and Homeland Security Investigations (UC-2) met and corresponded with PERSON-1 and others associated with OPPOSITION GROUP-1 regarding their desire to obtain weapons to effectuate a regime change in South Sudan. For example, in March 2022, PERSON-1 emailed a $13.5 million contract and purchase order—signed by PERSON-1 and an

[1] The cooperating defendant was charged in another District and pleaded guilty to Conspiracy to Commit a Violation of the AECA. He/she was allowed to cooperate pending sentencing and received a reduced sentence as a result of that cooperation.

OPPOSITION GROUP-1 leader and commander[2]—for the purchase of various munitions, including AK-47s, PKM rifles, and RPG-7 grenade launchers. This particular purchase, however, was not completed because PERSON-1 and his associates never provided the funds for the purchase.

35. In September 2022, UC-1 and UC-2 (collectively, the UCs) conducted an in-person, undercover meeting with PERSON-1 at a warehouse in Phoenix, Arizona. During the meeting, the UCs showed PERSON-1 several AK-47 assault rifles, PKM machine guns, 9mm pistols, RPG-7 grenade launchers, sniper rifles (with scopes), hand grenades, and ammunition. PERSON-1 also asked the UCs to invite several other individuals to participate in the meeting via Zoom, including a military general with a second South Sudan opposition group (OPPOSITION GROUP-2) and the general's U.S-based representative, an individual later identified as PERSON-2. During the Zoom meeting, PERSON-2 described their "rebel movement," including their "objective and goal of regime change in Juba" (the South Sudanese capital). UC-1 told PERSON-2 that UC-1 could procure the weapons and handle the transport logistics, but that there was "risk" associated with the deal because "South Sudan is an embargoed country." UC-1 further stated the U.S. government would not provide a license for weapons shipped from the United States to South Sudan, and there was "no legal way to do it." PERSON-2 and the other participants on the call acknowledged they understood. The UCs then showed PERSON-2 and the other participants the sample weapons,

[2] This individual has been designated by the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC) pursuant to Executive Order 13644 for threatening the peace, security, or stability of South Sudan and for expanding or extending the conflict or obstructing peace talks or processes in South Sudan.

and they discussed possible delivery methods. A few days after the meeting, PERSON-1 sent the UCs a revised purchase order for $3 million worth of weapons.

PERSON-2 Introduces Abraham Chol Keech to the UCs, and

Keech Continues Discussions Regarding Weapons Procurement

36. On February 20, 2023, the UCs conducted a follow-up video teleconference with PERSON-2, several generals associated with OPPOSITION GROUP-2 and a third South Sudan opposition group (OPPOSITION GROUP-3), and an opposition coordinator named **Abraham Chol Keech**. During the call, PERSON-2, who identified himself as a member of OPPOSITION GROUP-2, told the UCs he had briefed the call participants about the September 2022 meeting, including that the UCs were working to procure weapons to advance their movement to overthrow the current government in South Sudan. **Keech** told the UCs he is a U.S. citizen living in Utah, but was in an African country to mobilize forces on the ground. **Keech** said he had recently been in the South Sudanese capital (Juba) and believed the current government would collapse. **Keech** further stated to UC-1, "I'm sure you know the country is under sanction[s]," making it impossible for the current government to obtain weapons.

37. During the call, PERSON-2 discussed their desire to obtain weapons, but noted they did not have the money to do so. PERSON-2 proposed that a smaller order of between $25,000 and $50,000 worth of weapons and ammunition would help secure key areas in South Sudan near oil fields and gold mines. UC-1 explained that current U.S. sanctions prohibit the sale of weapons to South Sudan and organizations such as theirs. UC-1 said he was willing to violate U.S. laws—including by managing the logistics to get the weapons out of the United States—but that doing so would come at a risk to the UCs, their business, and anyone else involved. UC-1

added the weapons could be disguised as "humanitarian goods" or "machine parts" when shipped from the United States. PERSON-2 acknowledged that the UCs "[could] circumvent the sanctions" to deliver the weapons and suggested that he and **Keech** visit the UCs' facility and sign a deal once they received the "green light" from the military generals.

38. Following the call, UC-1 emailed PERSON-2 a price list for AK assault rifles, PKM machine guns, RPG-7 grenade launchers, sniper rifles, and associated ammunition, as well as an initial order for the $50,000 budget.

39. On February 25, 2023, UC-1 spoke with PERSON-2 by telephone. PERSON-2 told UC-1 that **Keech** would be soon returning to Utah and once he arrived, PERSON-2 would set up a face-to-face meeting in Phoenix with PERSON-2, **Keech**, and UC-1. PERSON-2 said they did not have any objections to the items listed in UC-1's email, and that **Keech** would bring the money for the purchase with him from Africa. PERSON-2 said he and **Keech** would create a list of weapons to inspect during the visit. UC-1 noted it would be good to build trust through the meeting because they are operating "outside U.S. regulations" and could not report to anyone if the deal falls apart. PERSON-2 agreed, saying "[w]e['re] coming there and meet face-to-face, no question about it." PERSON-2 also noted that while some of the other generals were skeptical (and thought the UCs were scammers), PERSON-2 believed they had established trust and a face-to-face meeting would aid the transaction.

40. On March 9, 2023, **Keech** texted UC-1 to arrange a meeting between **Keech**, PERSON-2, and UC-1. **Keech** wrote, "My name is Abraham **Keech**, I work with [PERSON-2]. We talked on Zoom few weeks ago while I was in [Africa]. I am now in USA and would like to

arrange for me and [PERSON-2] to meet with you on the price quotation. Best regards[,] Abraham."[3]

41. Over the next several months, **Keech** and UC-1 communicated by telephone, an encrypted messaging application, and in person, to discuss the procurement and smuggling of weapons and ammunition from the United States to South Sudan. Several of these communications are summarized below:

a. **March 12, 2023, telephone call with number ending in -1367:** During this call, **Keech** told UC-1 that he had spoken with "the guys on the ground" about the initial proposed order, and that ammunition was needed more than weapons. **Keech** further said he and PERSON-2 were coordinating a time to meet UC-1 in person, including to discuss "how the [weapons] would go there" (i.e., South Sudan), because of the "risk involved in actually shipping them." UC-1 asked **Keech** to identify a person or entity in another country (not South Sudan) that could accept the shipment, and **Keech** noted that air transport would be the best way to ship munitions within Africa. **Keech** and UC-1 agreed to discuss further when they met in person.

b. **April 10, 2023, in-person meeting:** UC-1 and UC-2 met with **Keech** and one of Keech's associates in Phoenix, Arizona (two generals also participated remotely). The UCs showed **Keech** AK assault rifles, machine guns, sniper rifles, and an RPG

[3] Based on database records, on March 8, 2023, **Keech** entered the United States on an itinerary that originated in an African country.

launcher. **Keech** agreed to provide the UCs with a detailed list of the weapons and ammunition needed (with a budget of $50,000 to $200,000) and to pay an initial deposit before returning to Phoenix at a later date to inspect the final shipment. **Keech** and the UCs also discussed potential shipment methods. **Keech** suggested that the UCs smuggle the weapons through a "U.S. military base in [AFRICAN COUNTRY-1]" to avoid "search[] by the [AFRICAN COUNTRY-1's] government." UC-1 noted that the U.S. military would not support this transaction, so they would have to sneak the shipment off the military base. **Keech** observed that only the first few shipments with the UCs would be "dealing with illegal business" and that subsequent shipments would be "legal" and could be made directly to Juba, intimating that after they successfully overthrew the current South Sudanese government, the sanctions barring U.S. shipments to South Sudan would be lifted and legal arms shipments could be completed.

c. **April 25, 2023, telephone call with number ending in -7731:** During this call, **Keech** told UC-1 that he and his associates were working to raise funds for the weapons purchase. In discussing smuggling options, UC-1 said he could smuggle the weapons onto a U.S. military base and that the "base [wouldn't] know anything about it." **Keech** said once the weapons arrive at the U.S. military base in AFRICAN COUNTRY-1, he would be able to smuggle them to South Sudan, possibly via a charter plane. They then discussed next steps, and **Keech** said he would work to collect the deposit money. **Keech** added that the funds would likely be transferred via bank wire and acknowledged that the transfer should not suggest

that the money was to purchase weapons and should instead be disguised as a payment for something else.

d. **October 16, 2023, telephone call with number ending in -7731:** During this call, **Keech** told UC-1 that the investors were concerned about the proposed shipping methods and the UCs' plan to get the items to the end destination. **Keech** said the investors wanted to explore alternative routes that did not involve a stop in AFRICAN COUNTRY-1. UC-1 told **Keech** the weapons could be shipped to a U.S. military base in AFRICAN COUNTRY-1 through UC-1's connections, and then leave the base disguised as humanitarian aid. **Keech** said he had explained this to the investors and would push for a virtual meeting so that UC-1 could explain it to them directly. UC-1 asked whether **Keech** thought he would be able to obtain funding from the investors. **Keech** asked UC-1 to talk on an encrypted messaging application.

e. **October 16, 2023, call via encrypted messaging application:** Shortly after the telephone call described above, UC-1 called **Keech** via an encrypted messaging application.[4] During this call, **Keech** told UC-1 he was working to organize supporters within South Sudan, and that the only thing preventing that was the

[4] The encrypted messaging application is linked to a user's telephone number and username. **Keech's** profile in the application is associated with his telephone number ending in -7731 and the username "Abraham Keech." Based on my training and experience, I know individuals often use encrypted messaging applications to obfuscate identities and make it more difficult for law enforcement to obtain records via legal process.

supply of weapons. **Keech** added that South Sudanese opposition leaders were talking to the White House and the U.S. Department of State. UC-1 reminded **Keech** that neither the White House nor the State Department would "approve us smuggling weapons through [AFRICAN COUNTRY-1]." **Keech** responded, "No, they will not," and clarified that they are seeking "political support," as well as support from private investors in Washington, DC. **Keech** also explained that a person in Washington named "Peter"—who is not a government official but is well connected—was not initially convinced that violence was the proper approach, but had since changed his mind. **Keech** said Peter knows that **Keech** had met with UC-1 and had seen the weapons, and Peter planned to meet with the financiers about funding.

Keech Introduces Peter Biar Ajak and They

Finalize the Weapons Purchase and Smuggling Plan

42. On November 3, 2023, UC-1 conducted a video call via an encrypted messaging application with **Keech** and an individual identified by **Keech** as Peter (**Peter Biar Ajak**).[5] **Keech** introduced **Ajak** as his partner, who was helping obtain weapons for South Sudan.

[5] The group video call was initiated by **Keech**. The group information identified "Peter" as **Peter Biar Ajak**, with a telephone number ending in -6747. In response to legal process, T-Mobile provided subscriber records for this telephone number. These records show that while the user did not provide a subscriber name or address, the device linked to this account has a Mobile Station International Subscriber Directory Number (MSISDN) name of "Peter Ajak." An MSISDN is a unique identifier assigned to each mobile device in a Global System for Mobile Communications network, and identifies a device during calls or data sessions.

43. **Ajak** told UC-1 he is not a U.S. citizen but lives in Washington, D.C. **Ajak** further stated that **Ajak**'s potential suppliers could not supply all of the weapons required by **Ajak**; as a result, **Ajak** was looking to UC-1 to supply the remaining weapons. UC-1 explained that facilitating a weapons purchase of this kind posed a legal risk for all of them because the U.S. Department of State prohibits U.S. persons or those residing in the U.S. from delivering weapons to South Sudan. UC-1 said their proposed purchase and export would be a violation of U.S. law, but that UC-1's company was willing to assume that risk in exchange for an additional fee and a pledge that UC-1's company would become the preferred vendor for **Ajak** and **Keech's** organization once they control South Sudan. **Ajak** responded he was aware of the sanctions and understood it would be a risk to UC-1, **Keech**, and himself, and they would therefore be discreet in conversations with others. UC-1 then explained to **Ajak** the proposed scheme, which he and **Keech** had discussed previously, i.e., smuggling the weapons to a U.S. military base in AFRICAN COUNTRY-1 and then smuggling them from AFRICAN COUNTRY-1 to South Sudan disguised as humanitarian goods (*see* ¶ 41(e), *supra*).

44. On November 8, 2023, the UCs conducted a videoconference with **Keech** and **Ajak** via an encrypted messaging application (*see* screenshot from the videoconference below, with **Ajak** on the left and **Keech** on the right).[6] During the videoconference, **Ajak** explained to the

[6] On November 8, 2023, **Keech** added username "Doctor Agutdau," associated with a telephone number ending in -3877, to an existing encrypted messaging application group with **Keech,** UC-1, and **Ajak's** telephone number ending in -6747. During this encrypted video conference, **Ajak** appeared on screen (with the name "Doctor Agutdau" appearing under his image). In a later encrypted message (dated January 3, 2024), **Ajak** confirmed he uses the username Doctor Agutdau. In response to legal process, T-Mobile provided subscriber records for the telephone

UCs that he is looking for "basically a coup … with both internal and external fronts" against the current South Sudanese government, which he described as corrupt, illegitimate, and beholden to foreign interest groups. He said he wanted to "knock it over and rebuild a new country," and that he would be installed as the new "Prime Minister" and "head of the government." He added his new government would be recognized by the United States and he "[has] the backing of the State Department, implicitly."[7]

---

number ending in -3877. These records show that the account has been active since October 1, 2023, and that the device linked to this account has a MSISDN name of "Peter Ajak." **Ajak** continued to use the Doctor Agutdau account to exchange encrypted messages with UC-1 regarding the smuggling of weapons to South Sudan for use in the planned coup.

[7] In September 2023, **Ajak** informed the U.S. Department of State that he was starting his own political party and considering a return to South Sudan to participate in elections. In October 2023, he and other members of ALLIANCE-1 met with the State Department and proposed that the State Department financially incentivize disillusioned South Sudanese military officers to convince the military to withdraw its confidence in the President of South Sudan as part of a peaceful process for leadership change in South Sudan. He did not mention procuring weapons or using violence. The State Department informed **Ajak** promptly and unequivocally that the State Department would not fund any proposals that called for non-democratic regime change, which **Ajak** acknowledged he understood.

45. During the video conference, **Ajak** stated he needed anti-tank weapons to disable the thirteen to fifteen functioning tanks in South Sudan. **Ajak** and **Keech** also asked the UCs about procuring anti-aircraft systems to disable the South Sudanese military's operational helicopters. They said they had a $100,000 budget for the purchase. UC-1 told **Ajak** and **Keech** there are sanctions in place prohibiting the sale of weapons to South Sudan and that their proposal was illegal. **Keech** responded, "[t]his issue of sanctions, don't worry about it." **Ajak** added that after the coup, the sanctions would be "lifted immediately," and **Ajak** was willing to execute a Memorandum of Understanding with the UCs "right now" to give the UCs the "assurance" that the UCs' company would be the official arms supplier to South Sudan after the regime change. UC-1 told **Keech** and **Ajak** to put together a list of approximately $75,000 worth of weapons—with an added $25,000 fee to account for the risk associated with the transaction—that would meet the buyers' $100,000 overall budget.

46. From November 9 to December 11, 2023, UC-1 sent **Keech** and **Ajak** a video and photos via an encrypted messaging application, showing the 7.62 x 39 mm and 7.62 x 51 mm ammunition and Stinger missiles that the UCs had procured:

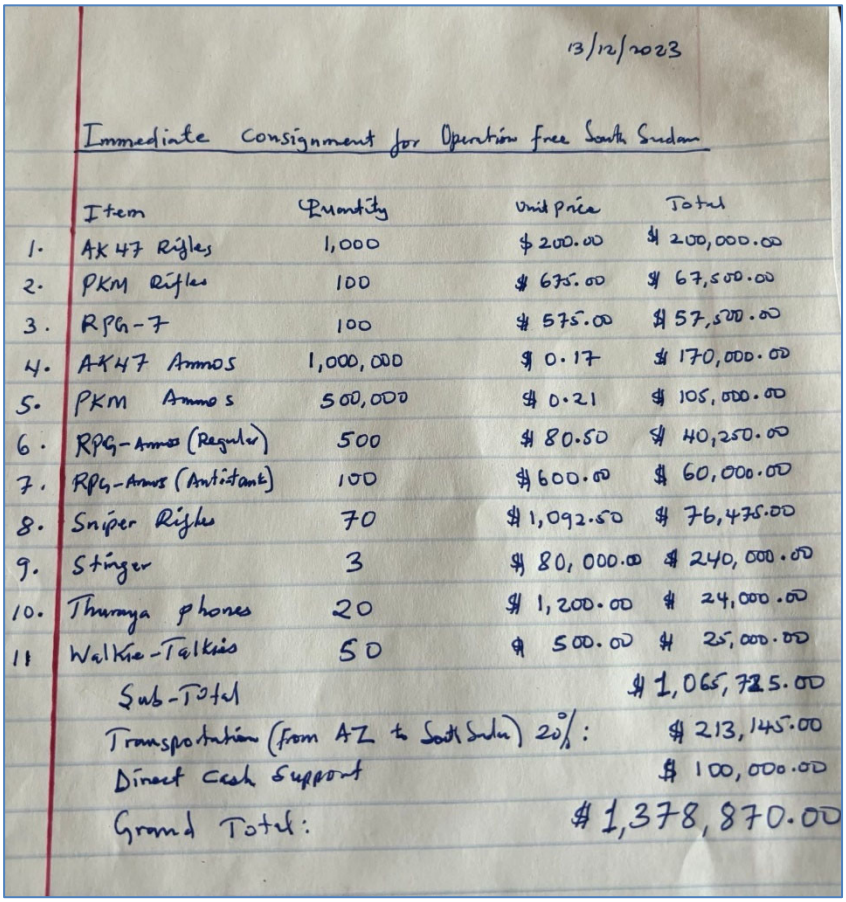
47. On December 13, 2023, UC-1 spoke with **Keech** on two separate calls via an encrypted messaging application. During the first call, **Keech** told UC-1 his most urgent needs were for AK-47 and PKM ammunition, RPG-7 high explosive and anti-tank rounds, and Stinger missiles. **Keech** explained that **Ajak** had met a potential new donor who would be able to pay in early January, either via cash or cryptocurrency. **Keech** also told UC-1 that he preferred that the weapons be transported from the United States to AFRICAN COUNTRY-1 via air transport, rather than by shipping container, because of the length of time associated with sea travel. During the second call, UC-1 told **Keech** he would add a 20% "shipping" fee to the cost of the total order to attempt to bribe U.S. military officials to allow the weapons onto (and later, off of) the U.S. base in AFRICAN COUNTRY-1.

48. On December 22, 2023, UC-1 spoke with **Keech** and **Ajak** via an encrypted messaging application. **Ajak** told UC-1 he wanted to better understand the proposed shipment

method and how UC-1 would avoid detection. UC-1 explained he had connections that would allow him to procure the weapons and then deliver them out of the country, including connections with U.S. personnel in AFRICAN COUNTRY-1, who in turn had connections with locals. UC-1 told **Ajak** and **Keech** they could disguise the weapons as humanitarian goods to get them off the U.S. military base. UC-1 added they could either (1) manifest and send the shipments as weapons and ammunition and then repackage them as humanitarian goods once in AFRICAN COUNTRY-1, or (2) disguise them as non-military goods from the beginning, which would negate the need for licenses or "fake paperwork" and reduce scrutiny. UC-1 further stated the proposed shipment scheme was "illegal because these things need a license to go and the United States is not sending anything to South Sudan." UC-1 added that if he were to transport the products by air (rather than by sea), the transportation costs would be higher because he would have to "pay off the guys." UC-1 emphasized the "U.S. military is not behind this," such a plan would be "completely unauthorized," and he would have to "pay[] off individual guys" for the plan to succeed. **Ajak** said air transport seemed to be the safer option, and that the faster the products made it to AFRICAN COUNTRY-1, the better, so long as the cost for air transport was not "exorbitant."

49. During the call, **Ajak** and **Keech** told UC-1 they would send UC-1 a list weapons to procure, with a budget of $1.28 million. This total budget included a 20% transportation fee. **Ajak** said his financiers would pay **Ajak** via a donation to his non-governmental organization (NGO), and **Ajak's** NGO would then wire the money to UC-1 from a U.S.-based bank account. **Ajak** said they would consider making a cash deposit but would need to "avoid surveillance as much as possible."

50. On December 22, 2023, **Keech** sent a photo to UC-1 and **Ajak** via an encrypted messaging application depicting a hand-written list of weapons for "Immediate consignment for Operation Free South Sudan." The weapons list included a $213,145 transportation fee (roughly 20% of the total cost).



13/12/2023

Immediate consignment for Operation free South Sudan

	Item	Quantity	Unit price	Total
1.	AK 47 Rifles	1,000	$ 200.00	$ 200,000.00
2.	PKM Rifles	100	$ 675.00	$ 67,500.00
3.	RPG-7	100	$ 575.00	$ 57,500.00
4.	AK47 Ammos	1,000,000	$ 0.17	$ 170,000.00
5.	PKM Ammos	500,000	$ 0.21	$ 105,000.00
6.	RPG-Ammos (Regular)	500	$ 80.50	$ 40,250.00
7.	RPG-Ammos (Antistank)	100	$ 600.00	$ 60,000.00
8.	Sniper Rifles	70	$ 1,092.50	$ 76,475.00
9.	Stinger	3	$ 80,000.00	$ 240,000.00
10.	Thuraya phones	20	$ 1,200.00	$ 24,000.00
11	Walkie-Talkies	50	$ 500.00	$ 25,000.00
	Sub-Total			$ 1,065,725.00
	Transportation (from AZ to South Sudan) 20%:			$ 213,145.00
	Direct Cash Support			$ 100,000.00
	Grand Total:			$ 1,378,870.00

51. Over the next few weeks, **Keech, Ajak,** and UC-1 continued communicating about the required weapons. For example, at various times, **Ajak** asked UC-1 to add two additional Stinger missile systems to the order, asked about the availability of javelin anti-tank weapons, and changed the "Buyer Information" on the purchase order from OPPOSITION GROUP-2 to an

alliance of South Sudanese political movements ostensibly working towards a free and democratic South Sudan (ALLIANCE-1). Based on my training, experience, and investigation to date, I believe that ALLIANCE-1 is the NGO referred to by **Ajak** during the December 22, 2023, call, when **Ajak** told UC-1 he would funnel money through an NGO and then on to UC-1 from a U.S.-based bank account.

52. On January 11, 2024, the UCs conducted a video teleconference via encrypted messaging application with **Keech** and **Ajak**. **Ajak** was observed sitting in a blue recliner in what appeared to be a residence. **Keech** appeared to be in a vehicle. During the call, **Ajak** told the UCs that he had a good meeting with his financier, who **Ajak** described as an individual interested in investing in South Sudan, and planned to meet the following week with the financier in Florida. **Ajak** told the UCs he had proposed to the financier that the financier pay the UCs directly from the financier's personal U.S.-based account, but the financier did not want it known that the financier was paying for weapons. **Ajak** asked the UCs whether they had another company that could disguise the purchase order and make it appear as if the financier was purchasing "furniture" or humanitarian aid instead. The UCs suggested they could create fake invoices for electronics, as well as a fake email train to support the ruse that the financier's purchases were for electronics (and not weapons and ammunition). That way, if the banks had questions about the transaction, the financier could produce records in support of the sale.

53. During the call, **Ajak** told the UCs that he had "discussed this at high-levels with [the] State Department," and had discussed the "need for a transition to take place in South Sudan" that **Ajak** and his colleagues would try to effectuate. He added, "The details, they don't want to know about it, we aren't discussing any details but they are aware generally speaking that we are going to do a nondemocratic transition in the country." He noted he and his colleagues are calling

it an "uprising" and not a "coup," and clarified that he had not told the State Department about the UCs' role or the weapons purchase. When UC-1 noted that what they are doing is in violation of several U.S. laws, **Ajak** reassured UC-1 that the only people who know of their efforts to smuggle weapons to South Sudan are **Ajak**, **Keech**, and the financier: "The part [the State Department] knows about is that we're going to do a regime change. No one close to U.S. government knows. No one else knows about our deal. There are people who know implicitly about our regime change. The only people who know are the three of us and the guy who will be paying."[8]

54. **Ajak** and UC-1 also discussed the budget for the weapons purchase. UC-1 explained that his transportation fee includes the actual transportation costs and the money required to "pay off" people to get the shipment out of the United States and from AFRICAN COUNTRY-1 to South Sudan. UC-1 added, "nobody is going to do [it] because it's not legitimate business, right, so we have to pay them off for the risk that they're taking."[9] **Ajak** asked UC-1 to reduce UC-1's smuggling fee to 18% or 19% (down from 20%) and give him a discount of around $100,000, noting he would be "extremely grateful" and "would remember this."[10] **Ajak** added,

[8] As discussed above, the State Department informed **Ajak** that the State Department would not fund any proposals that called for non-democratic regime change, which **Ajak** acknowledged he understood.

[9] Later in the conversation, UC-1 reiterated that even if the weapons were seized in Africa, the UCs and their company would be at risk in the United States. UC-1 explained that a portion of the total transaction price was a risk fee because the transaction was illegal and they are putting everyone's livelihood and freedom at risk.

[10] In negotiating a discount on the smuggling fee, **Ajak** noted, "[w]hen you bribe, you bribe one time, right?"

"We understand the risk," but if the UCs could lower the "delivery fee," **Ajak** may be able to pay the UCs within a week. They then made plans for **Ajak** and **Keech** to come to Arizona to inspect the weapons.

55. On January 17, 2024, UC-1 spoke with **Ajak** via an encrypted messaging application. **Ajak** said he had just met with his financier and others in New York City, New York,[11] who wanted to delay the purchase for six to eight months to allow more time to raise **Ajak's** profile as a South Sudanese opposition figure, conduct a public relations campaign, and improve intelligence gathering on South Sudanese government troop movements and foreign forces in South Sudan. The financier wanted the weapons procurement to be the "final part" of the preparation process. **Ajak** told UC-1 that in **Ajak's** view, they had a "specific window" to move the weapons into South Sudan: "What I tried to emphasize to [the others] was, the systems we have for delivery [rely] too much on the humanitarian aid, and that has a specific window, because humanitarian agencies are now stocking up during the dry season and this is where there is the large movement which would make it easy for these things to move in undetected. And then

---

[11] In a subsequent call with UC-1 on January 25, 2024 (discussed in more detail below), **Ajak** confirmed that the financier typically lives in Florida, but travels to New York City at least once a week, which makes meeting in New York more convenient. Thus, investigators believe that the January 17, 2024, meeting was with the same financier as the one referenced in ¶ 50, *supra*.

In addition, during the January 17 call, **Ajak** mentioned to UC-1 that a former U.S. military member and a former State Department official had participated in the meeting between **Ajak** and the financier to provide guidance regarding the coup. Based on my training and experience and the investigation to date, I believe that PERSON-5 and PERSON-4 are the former U.S. military member and former State Department official, respectively.

also because it's dry season, it's easier to move them from everywhere." **Ajak** added that given global demand for these products, he was worried the UCs would not be able to hold the products for six to eight months. UC-1 and **Ajak** then discussed options for holding the products in the United States, including a down payment of $1 million (possibly broken into separate payments). **Ajak** said he would speak again to the financier to discuss options and next steps.

56. Over the next few days, investigators learned that **Ajak** would be traveling to New York City for another meeting with the financier the following week.

57. At approximately 4:32 p.m., on January 23, 2024, Montgomery County Police Department ("MCPD") officers identified **Ajak** at the **PREMISES.** MCPD officers observed **Ajak** enter an Uber with a travel bag.

58. At approximately 5:48 p.m., on January 23, 2024, Amtrak Police Department ("APD") officers identified **Ajak** onboard Acela train 2122, in car 3, seat number 03C, bound for Penn Station in New York City.

59. HSI agents in New York City, who were assisting with surveillance, observed that on the afternoon of January 24, 2024, **Ajak** entered an office high-rise building. Based on information provided by the building's security company in response to legal process, **Ajak** checked into the building for a meeting called, "South Sudan Strategy Session," along with several other individuals, including PERSON-3 and PERSON-4. The meeting, which lasted approximately two-and-a-half hours, was held in a law firm's office.[12]

---

[12] Records from the building's security company indicate that **Ajak** met at the law firm's office on several other occasions, including on January 17, 2024, the date of his prior meeting with his financier (*see* ¶ 55, *supra*). PERSON-3, PERSON-4, and PERSON-5 also attended this meeting.

60. The day after the meeting, on January 25, 2024, **Ajak** spoke with UC-1 via an encrypted messaging application. During the call, **Ajak** said he had had a generally "good meeting" the day before. **Ajak** said he had met with a "middleman" in New York City who represents the financier. **Ajak** described the middleman as someone he has known for a long time and is a "very good friend." Based on my training and experience, and the investigation to date, I believe that the middleman referenced by Ajak is PERSON-3. **Ajak** said that during the meeting, they discussed the timeline and other details for the transaction, including:

- *Timeline:* **Ajak** said they wanted the weapons in Bor, South Sudan, by March 30, 2024.
- *Payment:* **Ajak** asked UC-1 to reduce the overall transaction price to $3 million (*see also* ¶ 54, *supra*).
- *Personal Use Items:* **Ajak** also asked UC-1 to procure a helmet, bulletproof vest, and rifle for his own personal use. He noted that "because I'm obviously going to be leading this mission," he needed "something really dependable and something that is easy and something that is pretty bad ass." UC-1 said he had sniper rifles on hand that **Ajak** could use, and **Ajak** said he wanted to shoot the rifle at a shooting range when he and **Keech** came to Phoenix to inspect the weapons prior to shipment.

61. **Ajak** said he had also set up a meeting with the middleman and the financier[13] for the following week in New York City. He added that his attorney would also participate in the

[13] **Ajak** noted that the financier typically lives in Florida, but travels to New York City at least once a week. He added that he and the financier have a "long, long relationship," and the financier has given **Ajak** money in the past, although prior investments have been in the $100,000 range.

upcoming meeting—when pressed by UC-1 about the presence of an attorney at the meeting, given the illegality of the transaction, **Ajak** assured UC-1 that the attorney is someone he fully trusts and is "fully invested" in the plan. **Ajak** noted that neither the attorney nor the middleman knew about UC-1 or UC-1's role in the transaction; they knew only that **Ajak** was procuring weapons for $3 million, but did not know (and did not want to know) any further details. He also added that while several generals remained involved with his plan, **Ajak** was the ultimate decision-maker on the purchase.

62. The following week, investigators learned **Ajak** would be traveling to New York City on February 8, 2024. HSI agents observed **Ajak** meet with PERSON-3 and another individual in a condominium building on 61st Street. The day after the meeting (February 9, 2024), **Ajak** spoke with UC-1 via an encrypted messaging application. During the call, **Ajak** told UC-1, "We are getting the funding," and the two discussed the payment and delivery schedule. **Ajak** expressed concern that "[i]f we pay you all the money and then you don't deliver, then we are fucked, right?" **Ajak** therefore agreed to pay a $1 million deposit (roughly one-third of the contract price) on or around February 19, followed by additional payments when the weapons shipped ($1 million), arrived in AFRICAN COUNTRY-1 ($500,000), and arrived in South Sudan ($500,000). **Ajak** reiterated they needed the weapons in South Sudan by March 30—when UC-1 said he planned to ship the weapons via sea cargo, **Ajak** observed that doing so would "help with the cost" and was also "less risky." **Ajak** also told UC-1 the payment would be made via a wire transfer

---

Ajak said the financier is not South Sudanese but is instead an economic investor who would like to sign a Memorandum of Understanding (MOU) with **Ajak** for later mineral investments in South Sudan.

from a U.S.-based bank account. He directed UC-1: "What you will need to do though, is we need to, like, bill it as, like, something that is more creative," such as "humanitarian whatever," or "humanitarian support for democracy." They further discussed adjustments to the purchase order (e.g., adding quantities) and made plans to conduct the weapons inspection on February 21, 2024, in Phoenix, Arizona.

63. On February 12, **Ajak** and UC-1 exchanged text messages via an encrypted messaging application. UC-1 sent **Ajak** an updated copy of the contract. In response, **Ajak** instructed UC-1 to prepare a (fictitious) invoice, saying: "[n]ow, prepare another invoice for humanitarian aid supplies of the equivalent amount."

64. Also on February 12, 2024, **Keech** spoke with UC-1 via an encrypted messaging application. **Keech** told UC-1 that his colleagues "on the ground" had identified other weapons suppliers, but **Keech** had told them they should work with UC-1's company as the only supplier. UC-1 thanked **Keech** and noted that the UCs view the deal as an investment for future business once the current government of South Sudan is overthrown. UC-1 noted that after the coup, these deals would be legal. **Keech** agreed, noting they "won't have to hide anything" and can work to procure larger items, including helicopters, that the country will need.

65. On February 13, 2024, UC-1 told **Ajak** via an encrypted messaging application that he "need[ed] a name of company or person for the invoice if you want it to look right." **Ajak** responded, "[t]he fake invoice?" and UC-1 replied, "[y]es." **Ajak** then responded with the name of a company ("U.S. Company-1"), saying "[t]hat's the company that will be paying you." **Ajak** also provided an address for the company. PERSON-4, the marketing and public relations specialist mentioned herein, is the Registered Agent for U.S. Company-1. The address provided by **Ajak** for the company is also a residence formerly associated with PERSON-4.

66. Later that day, **Ajak** spoke with UC-1 via an encrypted messaging application regarding the fake paperwork for the deal. UC-1 told **Ajak**, "I just want to get this fake invoice right"; **Ajak** explained that he had an MOU with his financier that contemplated "costs for contracting a company for security provision for field activities inside South Sudan and refugee camps." **Ajak** therefore instructed UC-1 that the invoice "should appear like costs for what a normal security company would need, to provide security inside a country that has hostilities." **Ajak** further directed UC-1 to "basically break that into, like, components of what does that mean"; in other words, if the UC company were really providing security in South Sudan, it would need to invoice for "personnel, you need to ship materials, you need whatever." "[T]he whole point," according to **Ajak**, was that he and his colleagues had "contracted your company to provide security for our humanitarian, human rights, and civic engagement in South Sudan, so the invoice should reflect that cost."

67. During the call, UC-1 asked **Ajak** whether the middleman (PERSON-4) sending the money (from the U.S.-based bank account) knew about UC-1's company. **Ajak** responded that the middleman "is someone who is working with me, primarily handling the PR, and is also providing me a cover so that the money doesn't necessarily come to my account." UC-1 then asked whether the middleman knows the UC company is "not really providing these services to him," to which **Ajak** responded:

Ajak: Yes, he knows, he knows what you're providing.

UC-1: He knows that we're providing the weapons.
Ajak: Right. But we just want to cover our bases with a paper trail.

Ajak added the middleman knew of the UCs' company, stating "I had to come clean with him because you know, he's doing me a huge favor." Shortly after the call, **Ajak** sent UC-1 a

message via an encrypted messaging application with language to use on the invoice: "Contract a company for security provisions for field activities related to human rights, humanitarian, and civic engagement inside South Sudan and refugee camps."

68. On February 15, 2024, **Ajak** spoke with UC-1 again regarding the arms shipment via an encrypted messaging application. **Ajak** told UC-1 that the "situation is so desperate right now in [South Sudan] that there might be a revolution while [the weapons] are stuck in the sea, and then we will miss out on the action." He asked UC-1 to revert back to a shipment plan that involved flying the weapons out of the United States, rather than shipping them by sea cargo. UC-1 reminded **Ajak** that if they fly the weapons to a U.S. military base in AFRICAN COUNTRY-1, that would mean "more people that I've got to pay off" on the base once the weapons land, which would increase the transportation costs. **Ajak** proposed removing some items from the order to make it financially feasible, telling UC-1 that although UC-1 "may not make a lot of profit" on this first weapons deal, the "profit will come when we succeed, my brother, think of this as an investment." **Ajak** added that money had been sent earlier that day from the financier to the middleman (PERSON-4)'s U.S.-based bank account, and the funds should be available in a few days. **Ajak** told UC-1 that his "first priority" when the money clears is to pay the UCs for the weapons. **Ajak** then directed UC-1 to update the "real contract" and "also the fake contract," so that he could send the "fake contract" to the middleman for payment. UC-1 confirmed, "[e]ven though [the middleman is] just getting the fake invoice, he's aware of the real deal that we're doing?" **Ajak** responded, "[y]es, he knows."

69. On February 16, 2024, **Ajak** and **Keech** spoke with UC-1 via an encrypted messaging application, both together and separately. In the first call (with both **Ajak** and **Keech**), **Ajak** expressed concerns that the UCs would be able to deliver the weapons as promised. He

noted that his "consulting team here in the U.S." worried the UCs might defraud him of his money and fail to supply the weapons.[14] During the call, **Ajak, Keech,** and UC-1 discussed the need by both parties to trust one other. UC-1, for example, reiterated to **Ajak** and **Keech,** "[w]hat we're doing does come with some inherent risk. … I have never misled you in the fact that there are risks, but that's why there's a premium that we're asking for payment." UC-1 added, "if I get caught, my business, I go to jail, [UC-2] and I go to jail, we lose everything that we've worked for."

70. **Ajak** told UC-1 that for his part, "[his] neck is on the line," because he has worked to obtain this "significant amount of resources" and if "this goes up in smoke[], that's a massive problem for [him]." **Ajak** added that he has to be careful and has to "look out for [him]self" and the "partners working with [him]." **Ajak** explained, however, that working with the UCs remained attractive, noting:

> We have another option of just buying within our neighborhood in Africa, [but] what makes your part of the deal attractive to us, is not just . . . what you can provide us for this current effort, but once we do succeed because we want to have access to American arms. [If able to] establish the next government in South Sudan, we want to increase our business with the United States and with American business people, [which is] part of what makes our relations with you attractive, otherwise we could easily buy from [AFRICAN COUNTRY-2] or from any of our neighboring countries that have hostility towards South Sudan and just truck it across the border. But we want to establish this long-term

[14] Later in the call, **Ajak** told UC-1 that "even our lawyers are asking" how he knows the UCs will not "run[] off" with the money. In a subsequent call between **Keech** and UC-1 later the same day, **Keech** explained that the advisors were worried because this was "an illegal deal, . . . if anything go[es] wrong we lose everything."

> relationship with you because we want to have access to certain systems that are only available in the United States.

71. **Ajak** and **Keech** then asked UC-1 to restructure the payment schedule so that they would pay the UCs $500,000 by February 20, 2024; pay an additional $1 million after inspecting the consolidated weapons and ammunition before air shipment to AFRICAN COUNTRY-1; pay another $2 million when the goods arrive in AFRICAN COUNTRY-1; and pay the remaining balance upon arrival in Bor, South Sudan. **Ajak** asked UC-1 to "make the revision to the fake invoice and put that payment schedule so that I can send it to [the middleman's company, U.S. Company-1] so they can make the initial transfer."

72. Later that day, UC-1 sent **Ajak** a copy of the revised weapons contract and the "fake" security provision contract, which included the agreed-upon payment schedule and delivery methods. With respect to the weapons contract, the parties agreed that the weapons would be sent via air cargo from the United States to AFRICAN COUNTRY-1, and then via truck convoy from AFRICAN COUNTRY-1 to South Sudan. The weapons contract also included language requested by **Ajak** via encrypted call and instant message, that the "parties agreed to honor the prices and the payment and delivery schedule as negotiated, and would allow no changes whatsoever to them, short 'an act of God.'" With respect to the "fake" security provision contract, the invoice included much of the language provided by **Ajak** via encrypted messaging application on February 13, 2024, regarding the nature of the services to be provided.

Weapons Contract (Excerpt):

CONTRACT

Immediate consignment for Operation Free South Sudan

Buyer: ALLIANCE-1

Seller: [redacted]

Destination: South Sudan

Contract number: [redacted]

	Item	Quantity	Unit Price	Total
1.	AK-47 Rifles (Full Auto)	1,000	$350.00	$350,000.00
2.	PKM Rifles	300	$675.00	$202,500.00
3.	RPG-7 launcher	200	$575.00	$115,000.00
4.	7.62x39 ammo	2,000,000	$.17	$340,000.00
5.	7.62x54 ammo	1,500,000	$.21	$315,000.00
6.	PG-7 HE round	1000	$600.00	$600,000.00
7.	PSL Sniper Rifle	70	$1092.50	$76,475.00
8.	FIM92 Stinger System	10	$80,000.00	$800,000.00
9.	Satellite phone	20	$1,200.00	$24,000.00
10.	Handheld Radio	50	$500.00	$25,000.00
11.	M67 Hand Grenades	500	$60.00	$30,000.00
12.	PG-7VT/PG-7T AT Round	500	$800.00	$400,000.00
13.	AN/PVS Monocular	10	$12,000.00	$120,000.00
			Subtotal-	$3,397,975.00
			Transportation-	$575,000.00
			Total -	**$3,972,975.00**

Payment Schedule:

1. $500,000 deposit for consolidation by February 20, 2024.
2. $1,000,000 upon inspection of consolidated shipment in U.S. no later than March 8, 2024
3. $2,000,000 upon inspection in [redacted] no later than March 15, 2024
4. $472,975.00 upon final delivery in Bor, South Sudan no later than March 20, 2024

Delivery Method: Air cargo to [redacted] from U.S. and truck convoy from [redacted] to Bor, South Sudan. If payment schedule is met, final delivery to Bor, South Sudan will be no later than 3 weeks from initial down payment.

The parties agreed to honor the prices and the payment and delivery schedule as negotiated, and would allow no changes whatsoever to them, short "an act of God."

"Fake" Security Provision Contract (Excerpt):

CONTRACT

Buyer: U.S. Company-1
N.Y. Address
C/O Dr. Peter Biar Ajak

Seller:

Destination: South Sudan

Contract number:

Line Item:

1. Consulting Services to Develop Security Provisions for Field Activities Related to Human Rights, Humanitarian, and Civic Engagement Inside South Sudan Refugee Camps.	$1,000,000.00
2. Items Required to Implement Activities Associated with Contingency Refugee Operations (to include but not limited to initial site surveys, communications equipment for associated personnel, access control equipment, perimeter fencing, traffic control equipment, fire suppression/prevention equipment etc.)	$1,000,000.00
3. Shipping, Installation and Training of Systems and Equipment.	$1,972,975.00
Total -	**$3,972,975.00**

Payment Schedule:

1. $500,000 deposit for consolidation by February 20, 2024.
2. $1,000,000 upon inspection of consolidated shipment in U.S. no later than March 8, 2024
3. $2,000,000 upon inspection in no later than March 15, 2024
4. $472,975.00 upon final delivery in Bor, South Sudan no later than March 20, 2024

Delivery Method: Air cargo to from U.S. and truck convoy from to Bor, South Sudan. If payment schedule is met, final delivery to Bor, South Sudan will be no later than 3 weeks from initial down payment.

Keech and Ajak Facilitate Transfer of

$500,000 and Meet UCs for Weapons Inspection

73. On February 19, 2024, **Ajak** sent UC-1 a message via an encrypted messaging application with a photo showing that $275,000 would be wired the following day to the UC's bank account. **Ajak** added that another $225,000 would be sent to the UCs on February 21, 2024, and explained, "We have to spread it out to avoid a bank review." He further stated, "We are doing it this way to avoid suspicion, which is good for you and us." On or about February 20, 2024, the UCs observed that a $275,000 deposit cleared in the UCs' Arizona-based bank account from U.S. Company-1. On or about February 21, 2024, another $225,000 deposit from U.S. Company-1 cleared in the account.

74. On February 22, 2024, the UCs conducted an in-person, undercover meeting with **Keech** and **Ajak**[15] at a warehouse in Phoenix, Arizona. During the meeting, the UCs showed **Keech, Ajak**, and PERSON-6 samples of AK-47 assault rifles, PKM machine guns, RPG-7 grenade launchers, sniper rifles, and other items. **Keech, Ajak**, and PERSON-6 handled and inspected the weapons; **Ajak**, in particular, tried on the bulletproof vest and helmet procured by the UCs, and handled two different rifles, stating "I've gotta be leading from the front, not the back."

---

[15] **Keech** and **Ajak** were joined by another individual, PERSON-6, an individual traveling on a Canadian passport. On February 17, 2024, **Ajak** sent a message to UC-1 via an encrypted messaging application describing PERSON-6 as an "associate of ours" who is a "weapon expert."

75. During the meeting, the UCs reiterated that the proposed export of weapons from the United States was illegal. At various times during the meeting, UC-1 told **Keech** and **Ajak:**

- "The reason that you're paying the premium … this all needs licenses by the U.S. government, that's where our services come in, we're not getting those and we're able to get [the weapons] out. South Sudan is restricted, for now."
- "The U.S. military has nothing to do with this, this is on us, we're paying somebody off to get it onto the base and airlifted out and arrive for you."
- "It's the business that we work in, … it's not legal … you can't take me to court right, I can't take you guys to court, … a lot if it is built on trust."
- "It's illegal, right, for these to be in [AFRICAN COUNTRY-1], I'm not getting a license for [AFRICAN COUNTRY-1]."

76. During the meeting, **Ajak** and **Keech** told the UCs that after consulting with an advisor, their previous doubts had been resolved. When asked what made them comfortable, **Ajak** responded, "I have a friend that is advis[ing] me, they're helping me with the whole process, and they assured me that no, don't worry [the UCs] know what they're doing." When asked which advisor **Ajak** had been talking to, **Ajak** responded, "You know the company that is paying you, that friend of mine. I trust him, he knows exactly what we're doing." When asked whether the advisor knew about the weapons systems, **Ajak** told UC-1 the advisor "is aware" and knew about the "fake invoice." UC-1 confirmed: "The guy from [U.S. Company-1] knows, the one who transferred it knows, that we're dealing with weapons out of the U.S.?" **Ajak** responded, "He knows." Later in the conversation, **Ajak** identified the adviser by his first name, which is a common derivate for the first name of PERSON-4. **Keech** was present for these discussions.

77. During the meeting, **Ajak** signed and initialed copies of both the weapons contract and the "fake" security provision contract excerpted above. **Ajak** further told the UCs, "Once we're able to succeed, we will … sit down and negotiate a … multi-year contract, because we're going to need to rebuild an Army and we're in a really bad neighborhood." UC-1 responded, "I would suspect that even after you overthrow the current government, sanctions will last still … so we can still supply you through the same things because we've got the logistics to get them through without a license." **Ajak** acknowledged that the sanctions may still be in place for a few years. UC-1 noted, "There's a premium on this obviously because of the risk that we're taking," including costs associated with "the people that we pay off to get it out, to smuggle it onto the military plane." UC-1 added that "all of that stuff comes at a cost," but "once you're able to just send it legally, we get all the licenses, we do all that, then, I can sleep a little bit soundly." **Ajak** said, "Once we succeed, [the United States] will be invested in … our support." He added that the United States is the "pen-holder on South Sudan at the [United Nations], so once the U.S. agrees to move to drop the sanctions," the sanctions may not be renewed.

78. At the conclusion of the meeting, the UC's took **Ajak**, **Keech**, and PERSON-6 to Phoenix Sky harbor Airport for their returns flight home. It was learned that **Ajak**'s flight landed at Ronald Reagan Washington National Airport at approximately 7:46 p.m. The distance between the airport to **PREMISES** is an approximately 30-40 minute drive.

79. At approximately 8:43 p.m., on February 22, 2024, an HSI agent observed a vehicle pull up at the **PREMISES**. The HSI agent observed a man fitting the physical characteristics of **Ajak** exit the vehicle as a passenger and retrieve luggage from the back of the vehicle. The person believed to be **Ajak** walked to the front door of the **PREMISES** and knocked several times. A person believed to be **Ajak**'s spouse and **Ajak** entered.

80. On February 23, 2024, **Ajak** and **Keech** spoke with UC-1 via an encrypted messaging application. UC-1 told **Ajak** and **Keech** that he was able to consolidate the weapons for an inspection on March 1, 2024. **Ajak** and **Keech** agreed to travel to Phoenix, Arizona, the following week for the inspection. With respect to payment, **Ajak** explained that "the maximum we can pay a day without raising bank suspicion is $225,000," and that "once it's above $225[,000], it triggers an immediate bank review." **Ajak** stated he would therefore initiate a series of wire transfers in the amount of $225,000 per day starting on February 26 and continuing to March 1, 2024.

Investigators Conduct License

Checks for Keech, Ajak, and ALLIANCE-1

81. On January 19, 2024, BIS conducted a license history check in the BIS licensing system. BIS has no licenses or license application history for PERSON-1, PERSON-2, **Keech, Ajak,** or **Ajak's** alias, Doctor Agutdau. Additionally, on January 19, 2024, BIS issued a License Determination for the 7.62 x 39 mm and 7.62 x 54 mm ammunition for export to the Republic of South Sudan. The ammunition has an Export Control Classification Number (ECCN) of 0A505.a, and on all relevant dates, ammunition exports to South Sudan were controlled for National Security, Regional Stability, and United Nations Embargo reasons. Accordingly, a BIS export license was required to export or re-export the ammunition to South Sudan. On February 6, 2024, BIS also issued a License Determination for a sniper rifle with scope, which has an ECCN of 0A501.a, and requires a license issued by BIS to be lawfully exported from the United States to South Sudan for National Security and Regional Stability reasons. As noted above, there is no license application history for PERSON-1, PERSON-2, **Keech, Ajak** or Agutdau.

82. On February 7, 2024, I received notification from DDTC that AK-47 rifles (fully automatic), PKM rifles (fully automatic), RPG-7 grenade launchers, and FIM-92 Stinger missile systems are classified as defense articles under the USML and require a license or other approval prior to export from the United States. Based on my training and experience, I also know that PG-7 HE rounds, M-67 hand grenades, and PG-7VT / PG-7T AT rounds are of the type controlled for export by DDTC and require a license issued by DDTC to be lawfully exported from the United States. On February 6, 2024, I received a notification from DDTC indicating that after a diligent search, DDTC found no record of any registration application, export license application, export license grant, or any other written approval provided to PERSON-2, **Keech, Ajak,** Agutdau, ALLIANCE-1, or variations of their names. There is therefore probable cause to believe the targets have not obtained the required export licenses, notwithstanding the policy of presumptive denial for export license applications for defense articles destined for South Sudan as outlined in section 22 C.F.R. Part 126.1 (w) of the ITAR.

83. I submit there is probable cause to believe that **Ajak** resides at **PREMISES**, and that there is evidence located at **PREMISES.** Specifically, back in October of 2022, an HSI agent mailed immigration status paperwork to **PREMISES** for **Ajak**. On one occasion **Ajak** was observed leaving his residence and followed to New York City where he conducted a meeting titled "South Sudan Strategy Session". On another occasion **Ajak** was observed arriving at his residence after attending an undercover meeting where he signed a contract for approximately $4 million USD for weapons to South Sudan which is an embargoed destination. Additionally, DHS immigration databases reflect **PREMISES** as **Ajak's** address of record. I have also has obtained various business records that show **Ajak** using **PREMISES** as his mailing address. In response to legal process, Apple provided records on or about February 8, 2024, to show **Ajak** having an

active iCloud account with the email of agutdau@gmail.com and the mailing address of the **PREMISES**. Wells Fargo provided **Ajak's** credit card account record, ending in 5143, reflecting **PREMISES** as the mailing address. The most recently provided credit card statement with the response listed **PREMISES** as the mailing address and was dated November to December of 2023. Wells Fargo also provided **Ajak's** savings account application, ending in 1504, which reflected **PREMISES** as **Ajak's** mailing address. Additionally, Paypal provided records for **Ajak's** Paypal account, ending in 3285, in November of 2023. **Ajak's** paypal account listed **PREMISES** as the "primary street address," and reflected a mobile login on October 31, 2023.

84. As discussed above, the UC's have communicated with both **Keech** and **Ajak** via telephone and encrypted messaging applications associated with cellular telephones. And when **Keech** and **Ajak** came to Phoenix, Arizona, for the February 22, 2024 meeting with the UCs, each brought two cellular telephones with them to the meeting. Data obtained from a tracking warrant obtained on a telephone number associated with **Ajak** indicates these cellular telephones have geolocated to the vicinity of **PREMISES** on a regular basis and during hours when a person would be present in their home.

85. Based on my training and experience, I also know that information stored on cellular telephones can be copied or transferred to other digital devices (such as computers, external hard drives, or servers). Based on my training and experience, I know that individuals engaged in this type of offense often communicate with co-conspirators using their phones, computers, or other internet connected devices, including through encrypted platforms like the ones used by **Keech** and **Ajak** in this case. Further, I know based on my training and experience that individuals engaged in this kind of criminal activity often maintain their devices and records (including financial records, receipts, notes, ledgers, mail, tax records, and other papers) where the

individuals can have ready access to them, including in their homes. For these reasons, I believe probable cause exists that evidence for this offense will be found at **Ajak's PREMISES**, including on electronic devices

86. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

87. *Probable cause.* I submit that if a computer or storage medium is found on the **PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

88. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES**, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous

to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a

computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

89. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

90. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

91. Because several people may share the **PREMISES** as a residence, it is possible that the **PREMISES** will contain storage media that are predominantly used, and perhaps

owned, by persons who are not suspected of a crime. If law enforcement reasonably determines that **Ajak** likely had access to or control over such storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

92. Based on the foregoing information, I request that the Court issue the proposed warrants authorizing the search of the **PREMISES**, as described in Attachments A, for evidence, fruits, and/or instrumentalities of the **TARGET OFFENSES**, as described in Attachment B.

REQUEST FOR SEALING

93. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Date: February 28, 2024

Respectfully submitted,

Jeremy Kiser
Special Agent
U.S. Department of Homeland Security

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 28th day of February, 2024.

The Honorable Ajmel A. Quereshi
United States Magistrate Judge
District of Maryland

ATTACHMENT A

Property to be Searched

The property to be searched is 10106 Bosworth Ct., Bethesda, Maryland 20817 (the "**PREMISES**"), further described as a two-story brick townhouse style home with dark colored siding on the second story, one bay window to the left of the front door, and three single windows on the second story. House numbers depicting 10106 can be observed above the front door.

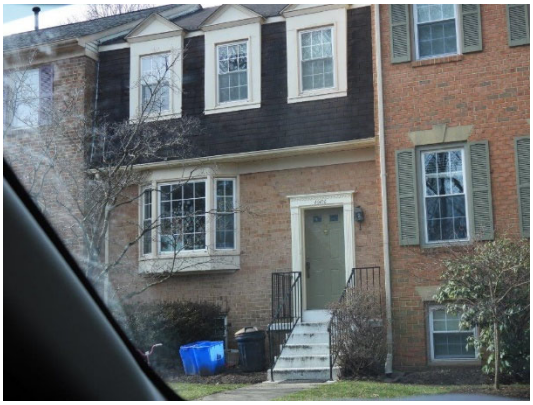


Figure 1 Front of Premises

ATTACHMENT B

Property to be Seized

1. All information, documents, photographs, videos, records, or communications relating to violations of (1) Conspiracy to Violate the Armed Export Controls Act and the International Traffic in Arms Regulations (22 U.S.C. § 2778(b)(2), (c); 22 C.F.R. §§ 121.1, 123.1, 126.1 127.1(a)(4), 127.3; (2) Conspiracy to Violate the Export Control Reform Act and the Export Administration Regulations (50 U.S.C. § 4819(a)(1), (a)(2)(D), and (b); 15 C.F.R. §§ 736.2(b)(1), 774, Supp. No. 1; or (3) Smuggling of Goods from the United States (18 U.S.C. § 554(a)) (the "**TARGET OFFENSES**"), involving **Peter Biar Ajak**, including information, in any format, pertaining to the following matters:

a. Documents, records, information, photographs, videos, or communications related to the violation of, or the attempt or conspiracy to violate, U.S. export laws;

b. Documents, records, information, photographs, videos, or communications related to the purchase, procurement, financing, transfer, shipment, delivery, or transshipment of weapons, ammunition, and/or other export-controlled items;

c. Documents, records, information, photographs, videos, or communications related to a change in leadership or government in South Sudan;

d. Documents, records, information, photographs, videos, or communications with representatives from any U.S. department or agency related to South Sudan;

e. Documents, records, information, photographs, videos, or communications related to **Ajak**'s (or his co-conspirators') knowledge of U.S. export control laws, including any license or registration applications;

f. Documents, records, information, photographs, videos, or communications related to domestic or international travel, including past and future travel documents, itineraries, tickets, visas, and passports;

g. Documents, records, or information related to the occupancy, residency, rental, ownership, or use of the **PREMISES**, including utility and telephone bills, rental, purchase or lease agreements, keys, and records of real estate transactions;

h. Documents, records, information, photographs, videos, or communications related to the identity or location of collaborators co-conspirators;

i. Evidence indicating **Ajak**'s state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation; and

j. The purchase, creation, possession, or use of physical or electronic accounts, or other access to computer systems, financial accounts, encrypted messaging applications, or social media platforms.

2. Any digital devices -- to include computers -- or other electronic storage media and/or their components that may constitute instrumentalities of, or contain evidence of the **TARGET OFFENSES** under investigation, including:

a. any digital device or other electronic storage media used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, or optical scanners;

b. any magnetic, electronic, or optical storage device capable of storing data, such as USB devices, SD cards, CDs, DVDs, optical disks, smart cards, PC cards, electronic notebooks, and personal digital assistants;

c. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

d. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

e. any physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices, or data; and

f. any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the digital device or other storage device was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the use of the device;

e. evidence indicating the digital device or other storage device user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the digital device or other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

h. evidence of the times the digital device or other electronic storage media was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

j. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

k. documentation and manuals that may be necessary to access the digital device or other storage device or to conduct a forensic examination of the device; and

l. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of an Internet Protocol ("IP") address to communicate with the internet, including:

a. records of IP addresses used; and

b. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorited" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

5. Safes or other locked storage containers that may contain any of the items referenced herein, as well as keys or other items used to access such containers.

6. Any U.S. or foreign currency exceeding $5,000.

7. This warrant authorizes the search and forensic analysis of electronic devices containing the foregoing evidence if:

a. The electronic devices in or within reasonable proximity to a container containing other evidence associated with **Ajak**;

b. The electronic devices are found within rooms known or discovered to be used by **Ajak**;

c. A person inside the premises advises officers executing the warrant that the electronic devices were used by **Ajak**;

d. Officers reasonably believe the device was utilized in connection with the use of an electronic device falling into one of the three categories listed above.

8. This warrant does not authorize the search or forensic analysis of electronic devices that do not fall within the scope of the preceding paragraph.

9. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

10. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

As used above, the term "storage device or medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

11. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent

reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.